

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-268125
(43)Date of publication of application : 28.09.2001

(51)Int.CI. H04L 12/56
G09C 1/00
H04L 12/28
H04L 12/66

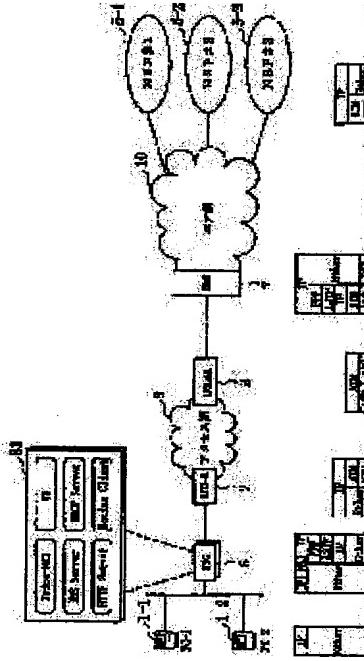
(21)Application number : 2000-081569 (71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>
(22)Date of filing : 23.03.2000 (72)Inventor : NAKAGAWA KOICHI
KANO MASAO
HAYASE KAZUYOSHI

(54) SELECTIVE VPN CONNECTION GATEWAY, AND COMMUNICATION METHOD USING THE GATEWAY

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a service for performing the on-demand selection of a connection destination and simultaneously connecting plural computers of a user side LAN with plural NSP.

SOLUTION: This gateway is provided with a DNS function 6-4 for detecting address solution and address overlap, a Twice-NAT function 6-5 for translating a transmission source address and a transmission destination address, a virtual router function 6-6 having logically independent plural router functions, an HTTP server function 6-2 and a Radius Client function 6-3. When there is the overlap with the SA of a transmission destination IP packet, while detecting the overlap of the IP address with the connection destination network, D/A conversion is performed as well and while using a VR 6-6-1 selected with the SA of a user terminal as a reference, a packet is routed to requested connection destination NSP 5-1, 5-2 and 5-3.



LEGAL STATUS

[Date of request for examination] 20.11.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3656134

[Date of registration] 18.03.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-268125

(P2001-268125A)

(43)公開日 平成13年9月28日(2001.9.28)

(51)Int.Cl. ⁷	識別記号	F I	テマコード(参考)
H 04 L 12/56		G 09 C 1/00	6 6 0 E 5 J 1 0 4
G 09 C 1/00	6 6 0	H 04 L 11/20	1 0 2 D 5 K 0 3 0
H 04 L 12/28		11/00	3 1 0 D 5 K 0 3 3
12/66		11/20	B 9 A 0 0 1

審査請求 未請求 請求項の数3 OL (全8頁)

(21)出願番号	特願2000-81569(P2000-81569)	(71)出願人	000004226 日本電信電話株式会社 東京都千代田区大手町二丁目3番1号
(22)出願日	平成12年3月23日(2000.3.23)	(72)発明者	中川 広一 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
		(72)発明者	加納 正雄 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内
		(74)代理人	100077274 弁理士 磐村 雅俊 (外1名)

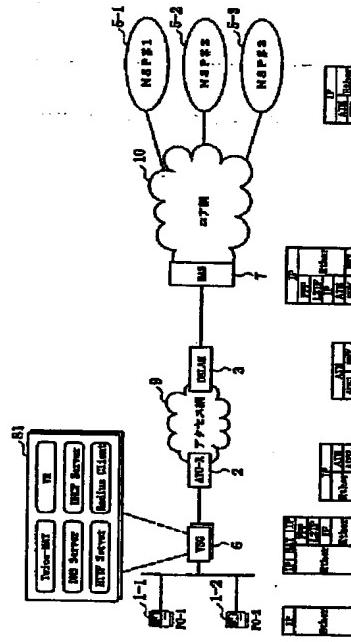
最終頁に続く

(54)【発明の名称】 VPN選択接続ゲートウェイおよびそれによる通信方法

(57)【要約】

【課題】接続先のオンデマンド選択と、ユーザ側LANの複数のコンピュータが複数のNSPと同時に接続するサービスを実現する。

【解決手段】アドレス解決とアドレス重複を検出するDNS機能6-4と、送信元アドレスおよび送信先アドレスを変換するTwice-NAT機能6-5と、論理的に独立した複数のルータ機能を持つ仮想ルータ機能6-6と、DHCP機能6-1と、HTTPサーバ機能6-2と、Radius Client機能6-3とを備え、接続先ネットワークとのIPアドレスの重複を検出しながら、送信先IPパケットのSAと重複があった場合にはDAの変換を行い、ユーザ端末のSAを基準に選択するVR6-6-1を用いて要求された接続先NSP5-1, -2, -3へパケットをルーティングする。



【特許請求の範囲】

【請求項1】 HTTPサーバとして機能する手段と、DHCPサーバとして機能する手段とを有する選択接続ゲートウェイにおいて、ユーザ端末からの接続要求に基づいて、送信元アドレスおよび送信先アドレスを変換するTwice-NAT変換手段と、論理的に独立した複数のルータとして機能する仮想ルーティング手段とを備えたことを特徴とするVPN選択接続ゲートウェイ。

【請求項2】 ユーザ端末からの接続要求に基づき、接続先ネットワークのDSNサーバに問い合わせを行い、該問い合わせに対する回答からIPアドレスの重複を検出し、重複がある場合には、接続先端末のIPアドレスを未使用のIPアドレスに変換して、該変換されたIPアドレスをテーブルに登録し、接続先ネットワーク内の端末のIPアドレスとして前記ユーザ端末に通知し、ユーザ端末から接続先ネットワーク宛の上りパケットの送信元アドレスを接続先ネットワークが該ユーザ端末に配布したIPアドレスに変換し、かつ前記重複のないアドレスに置換し、複数のルーティングテーブルにより、論理的に独立した複数のルートを選択して該パケットを送出することを特徴とするVPN選択接続ゲートウェイによる通信方法。

【請求項3】 請求項1に記載のVPN選択接続ゲートウェイにおいて、前記各手段に加えて、ユーザ端末が起動する該ユーザ端末にIPアドレスを配布する手段と、接続先ネットワークを切り替えるためのGUIを提供する手段と、接続先ネットワークのRASに問い合わせる認証手段と、PPP接続を行うための手段とを備えたことを特徴とするVPN選択接続ゲートウェイ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ADSL等の常時接続型アクセス系において、同一LAN内の複数のユーザ端末が同時に複数のNSP (Network Service Provider) への接続を可能にするVPN選択接続ゲートウェイおよびそれによる通信方法に関する。

【0002】

【従来の技術】 従来より、既存の電話回線を利用して、電話と共に映像伝送等のサービスを行うADSL (Asymmetric Digital Subscriber Line) 技術が知られている。例えば、米国の電話会社では、ADSL技術とデジタル映像圧縮技術のMPEG1を利用して、電話サービスと一緒に映像等を呼び出して視聴できるビデオオンデマンドがあ

る。一方、公衆網を専用網のように利用できるサービスとしてVPNサービス (Virtual Private Network Service) (仮想私設網) が注目されている。すなわち、加入電話網をあたかも社内の内線電話のように利用でき、例えば2~7桁の任意の電話番号を設定し、その番号で自由に電話できるようになる。これは、音声ネットワークのみならず、インターネットでもVPNサービスを提供する事業者 (例えば、NSP (Network Service Provider)) が出ている。

【0003】 図6は、従来における常時接続ネットワークのシステム構成図である。ADSL等の常時接続アクセス系におけるネットワークのシステム構成は、図6に示すように、ユーザ端末1-1, 1-2からADSLモデム(ATU-R)2を経由してアクセス網9に接続され、さらにDSLAM (Digital Subscriber Line Access Multiplexer (デジタル加入者回線アクセス多重化装置)) 3とATMスイッチ4を経由してコア網10に接続され、ATMスイッチ4を経由して接続先NSP5-1, 5-2に接続される。ATU-R (ADSL Transceiver Unit-Remote (ユーザ宅内側のADSLモデム)) 2は、8に示すように、NAT機能とDHCPサーバ機能とHTTPサーバ機能とを備えている。例えば、ユーザ端末1-1からNSPまたは企業LANのネットワーク5へ接続するためには、コア網にあるATMスイッチ4よりユーザが契約時に登録を行ったネットワークに固定的に設定され、契約ネットワークに接続される。ユーザ端末1-1から送信されたパケットは、ATU-R2からADSL網9を通り、一旦はDSLAM3で終端された後、ATMスイッチ4により当該ネットワークに転送される。

【0004】 なお、ネットワークの各ノードの下方に示す記号は、該当する位置にあるノードが備えているプロトコルスタックであって、レイヤーごとのプロトコル変換を示している。なお、DHCP (Dynamic Host Configuration Protocol) サーバは、TCP/IPを利用して通信する場合に、コンピュータにIPアドレスやデフォルト、ゲートウェイのアドレスを設定する必要があり、これを自動化するためのプロトコルとして、DHCPサーバ上にIPアドレスやデフォルト・ゲートウェイのアドレスを登録しておく。また、HTTP (Hyper Text Transfer Protocol) サーバは、WWWブラウザとファイル等の情報を送受信するために用いるプロトコルを備えたサーバである。このような構成では、契約時に登録を行ったネットワークに固定的に設定されているため、ユーザの希望する複数のネットワークをオンドマンドで選択することができないのは勿論のこと、複数のユーザ端末がそれぞれ異なるネットワークに接続

することもできない。

【0005】

【発明が解決しようとする課題】前述のように、従来のADSL等の常時接続アクセス系では、契約時に登録を行ったネットワークに固定的に接続されてしまうため、接続先の選択を行ったり、同時に複数端末により接続先を選択して希望する企業またはNSPに接続することができないという問題があった。

【0006】そこで、本発明の目的は、これら従来の課題を解決し、ADSL等の常時接続アクセス系を利用したコンピュータ通信において、接続先のオンデマンド選択（以下、選択接続サービスと記す）と、ユーザ側LANの複数のコンピュータが複数のNSPと同時に接続するサービス（以下、同時選択接続サービスと記す）とを実現することができるようなVPN選択接続ゲートウェイおよびそれによる通信方法を提供することにある。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明のVPN選択接続ゲートウェイは、ユーザ側に設置する装置として、アドレス解決とアドレス重複を検出するDNS機能と、送信元アドレス（SA）および送信先アドレス（DA）を変換するTwice-NAT機能と、論理的に独立した複数のルータ機能を持つ仮想ルータ（VR）機能と、さらにDHCP機能、HTTPサーバ機能、Radius Client機能を備え、これらを組み合わせることにより接続先ネットワークとのIPアドレス重複を検出しながら、送信先IPパケットのSAと重複があった場合のDAの変換も行い、ユーザ端末のSAを基準に選択するVRを用いて、要求された接続先NSPへパケットをルーティングする。これにより、ユーザPCと接続NSP内のPCのIPアドレスの重複を許容しながら、複数の接続先に任意に、かつ同時に接続することが可能になる。

【0008】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。

（第1の実施例）図1は、本発明の第1の実施例を示すネットワーク構成のシステム構成図であり、図2は図1におけるVSG（VPN Selection Gateway）のパケット処理の説明図である。第1の実施例では、VSG6とADSLモデム(ATU-R)2とが別個に設けられた場合を示しており、第2の実施例のように、両者が一体化されていない。図1に示すように、第1の実施例では、アクセス網9のADSLモデム(ATU-R)2の前段階に、81に示すように、Twice-NAT機能、VR機能（仮想ルータ機能）、DNS（domain Name System Server）サーバ機能、DHCPサーバ機能、HTTPサーバ機能およびRadius Client機能を備えたVSG6を設置したことを特徴としている。なお、D

NSサーバは、アドレス解決を行うサーバであり、Twice-NATのNATとは、基本的にSA（Source Address）のみをPrivate \leftrightarrow Globalの変換を行うが、Twice-NATはSAのみならず、DA（Destination Addresses）についても、変換を行う。NATの場合には、接続先のアドレス空間がGlobalなものを想定している。接続先が社内LAN等で、プライベートアドレスを用いている場合には、宅内LAN側のプライベートアドレス空間とコンフリクトを起こす場合がある。そのため、SAのみならず、DAについても、アドレス変換を行い、アドレスがコンフリクトしないようにする。DNS（Domain Name System）機能は、TCP/IPネットワークでは、ドメインと呼ぶ論理的なグループを階層的に設定でき、論理グループ名称であるドメイン名をコンピュータの名前の一部に組み込んで利用している。DNSサーバは、ホスト名とIPアドレスの対応表を持っている。また、Radius Client（Remote Authentication Dial-in User Service Client）は、アクセスサーバ経由で送られてくるユーザIDとパスワードを、ユーザ情報の管理テーブルと突き合わせて認証の可否を、アクセスサーバに伝える。このサーバは、ユーザ毎にアプリケーション・サーバのアクセス権限を与えたり、課金情報を収集するなどの管理用サーバである。

【0009】図1では、パソコンPC1-1がNSP#1のPC（図示省略）と通信し、PC1-2がNSP#2のPC（図示省略）と通信する例を示している。そのため、複数同時選択サービスを行うためには、複数のPPPセッションを張る必要があり、そのためにL2TPを用いている。PPP（Point to Point Protocol）は、2点間を接続してデータ通信する場合に利用するWAN用プロトコルである。ユーザPC1-1から送られたIPパケットは、SAによりVRが選択され、DHCPサーバにより割り当てられたプライベートアドレスをNAT機能を用いて、NSPから割り当てられたアドレスに変換する。DNSサーバにより接続先PCとIPアドレスの重複が検出された場合には、DAについても変換を行う。変換されたパケットは、指定のVC（Virtual Channel）を通じてNSPに転送される。これと並行して、他のユーザPCが他のNSPに接続要求する場合には、SAを確認して、異なるVRを選択するために、複数のPCが同時に複数のNSPに接続することが可能になる。

【0010】図2では、VSGにおいて、同時選択接続のためのパケット処理が行われる状態を示している。図2において、6はVSG、6-1～6-4はVSG6内に実装されたDHCPサーバ機能、Radius Client機能、HTTPサーバ機能、およびDNSサー

バ機能を示している。6-5～6-9はVSG内の参照テーブルであり、詳細には、SA-VR対応テーブル6-5、VR(仮想ルータ)6-6、アドレス変換テーブル(プライベート側)6-7、アドレス変換テーブル(グローバル側)6-8、およびARPテーブル6-9である。6-10はL2TP、7はダイアルアップだけでなく、ADSLやATMを収容するためのアクセスサーバであるBAS(Br adband Access Server)を示している。PC1-1, 1-2, 1-3の電源を投入すると、VSGのDHCPサーバ6-1からIPアドレスを取得する。なお、ここでは、DHCPサーバがPC1-1, 1-2, 1-3に与えるIPアドレスは、RFC1918に定められた任意のクラスのプライベートアドレスとする。

【0011】図3は、本発明の第1の実施例を示すVPN選択接続ゲートウェイの動作シケンスチャートである。PC1-1は、予めDHCPにIPアドレスを要求し(101)、DHCPサーバ6-1からIPアドレスを取得する(102)。PC1-1, 1-2, 1-3がWebブラウザを用いてHTTPサーバ6-2に接続し(103)、サーバ6-2からNSP選択画面が表示されることで(104)、GUI(Graphical User Interface)により接続先NSPを選択し(VR決定)(105)、ユーザ名、パスワードを入力してRadius Client6-3が選択した接続先NSPの認証サーバに認証要求を送出して(106)、認証を行う(108)。なお、認証動作は、接続先ネットワークのRAS(Remote Access Server(ダイアルアップユーザを収容し、コア網へパケットを転送する装置))に問い合わせる。ユーザの認証が行われた場合、SA-VR対応テーブル6-5の選択VR名フィールドにPCの送出パケットのSAと対応付けられた接続NSP用のVR名が設定される(109)。例えば、SA:a→VR名:VR1に、SA:b→VR名:VR2に、それぞれ変換される。同時に、NSP側から割り当てられたIPアドレス(Ga)とPC1-1に割り当てられているプライベートアドレス(a)を対応付けるアドレス変換テーブル6-7を生成する(110)。PC1-2についても、同様に生成する。PC1-1, 1-2が行ったARPテーブルの処理からPCのIPアドレスとMACアドレスを対応付けたARPテーブル6-9の生成を行う(111)。

【0012】次に、PC1-1がNSP#1にIPパケットを送出する処理手順を述べる。NSP#1のPC5-1-1と通信するPC1-1は、PC5-1-1の名前からそのIPアドレスを解決するために、DNSのqueryパケット(Requestパケットに対する返答)をVSG6のDSNサーバ6-4に送信する(112)。VSG6は、VR6-6-1により指定されている接続先NSP5-1のDNSサーバ5-1-2へ、P-

C1-1からのDNS queryをフォワードする(113)。NSP#1のDNSサーバから、PC5-1のDNSサーバから、PC5-1-1のIPアドレス(a')がresponseとして返送される(114)。なお、「a」と「a'」とは同じIPアドレスである。ところが、ここでPC1-1とPC5-1のIPアドレスが共に「a」となって、重複が発生する。そこで、DNSサーバ5-1-2は、PC5-1-1のIPアドレス(a')を他の任意のアドレス(Ge)に変換し、VR6-6-1のアドレス変換テーブル(グローバル側)6-8にそのマッピングを追加する(115)。【0013】このように変更されたDNSのresponseパケットをPC1-1に送信する(116)。これで、PC1-1の中では、PC5-1-1のIPアドレスは‘Ga’と記憶される。今後、PC1-1からPC5-1-1宛に送信されるIPパケットは、SA:a、DA:Geとして送信されることになる。送信されたパケットは、VSG6においてパケットのSAから適切なVRが選択され、SAとDA双方の変換を行う(117, 118)。すなわち、SA:a→Ga、DA:Ge→a'に変換される。この変換により、パケットはアドレスGe宛のものとして、L2TPトンネリング6-10を用いてPPP#1を通り、DSLAM3およびBAS7を経由してコア網10に送出される(図1参照)。

【0014】NSP#1のPC5-1-1から送出されるパケット(119)は、PPP#1を通りVSG6に送出され、VSG6においてSAとDAの変換が行われる(SA:a'→Ge、DA:Ga→a)(120)。そして、ARPテーブル6-9を参照してPC1-1に送信される(121)。同時に、PC1-2がNSP#2と通信を行うことも可能である。PC1-2はNSP#2を選択したものとする。全てのテーブルは、図4のシケンスチャートに示すように設定され、PC1-2とその他のPCからの送信データは選択VRが異なるため、送出先VC(Virtual Channel)がPC1-1とは独立している。そのため、PC1-1からの送出データとPC1-2からの送出データとが混同されるという問題は生じない。

【0015】(第2の実施例)図4は、本発明の第2の実施例を示すネットワークの構成図であり、図5は、図4において、ATU-R機能を内蔵したVSGを用いた常時接続ADSLネットワークの図である。なお、本実施例では、PPPoE over ATMを用いているが、IP over ATMでも同様に行うことができる。第2の実施例では、VSGとATU-R機能を一体化した構成のVSG6aを用いた場合を示している(図4の82参照)。この場合には、第1の実施例とは異なって、VSGとATU-Rの間のインターフェイスによる制約がないため、ADSLのATMインターフェイスに直接パケ

ットを転送することができる。すなわち、ATM上で、複数VC (Virtual Channel) を張ることができるため、図1で示したようにPPPセッションを複数張るためL2TPプロトコルを用いる必要がない。また、図5のVSG内の構成についても、図2におけるL2TP6-10の代りにATU-R機能6-11が配置されている。それ以外の構成は、ほぼ同一である。IPパケットの送出処理シーケンスに関しては、図3に示す第1の実施例と同じであるが、VR (仮想ルータ) には送出先VC (Virtual Channel 1) が記述されており、IPパケットVCを経由してBAS7まで転送される点で異なっている。

【0016】

【発明の効果】以上説明したように、本発明によれば、DNSサーバ機能、HTTPサーバ機能、Radius Client機能、DHCPサーバ機能、SA+VRルーティング機能を実装したVPN選択接続ゲートウェイを設けることにより、ユーザ側LANと接続するNSPのアドレス重複が発生するがないため、複数のコンピュータが複数のNSPに同時に接続することが可能になる。

【図面の簡単な説明】

【図1】本発明の第1の実施例を示す常時接続ADSL

ネットワークの構成図である。

【図2】図1におけるVSGの詳細構成図である。

【図3】本発明の第1の実施例を示すADSLネットワークによる動作シーケンスチャートである。

【図4】本発明の第2の実施例を示す常時接続ADSLネットワークの構成図である。

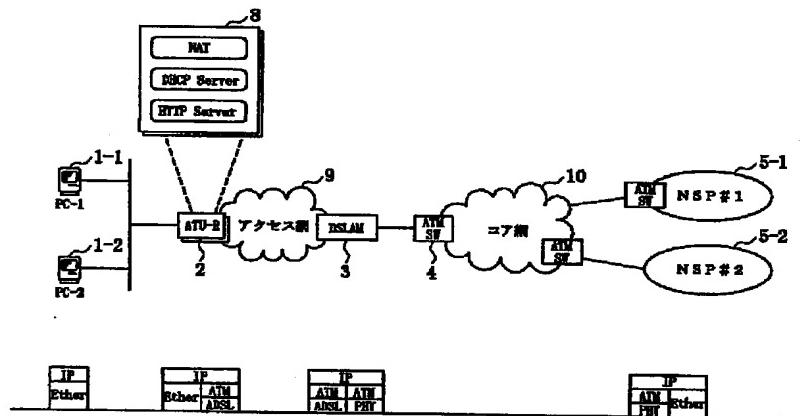
【図5】図4におけるATU-R機能を内蔵したVSGの詳細構成図である。

【図6】従来における常時接続ネットワークの構成図である。

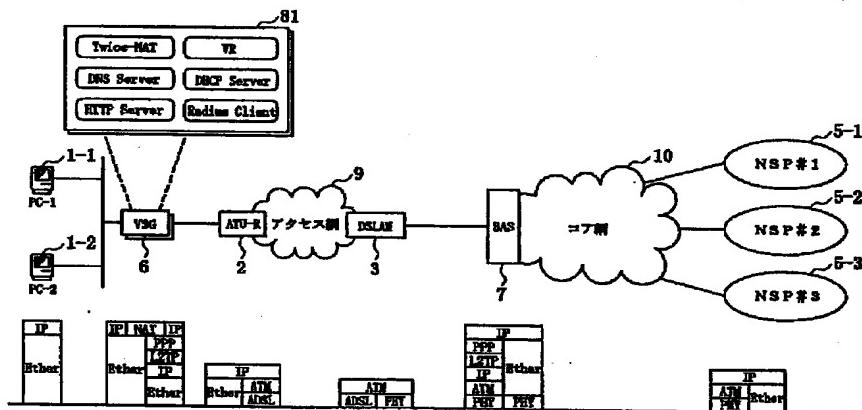
【符号の説明】

1-1, 1-2, 1-3…ユーザPC、5-1-1…NSPのPC、2…ATU-R (ADSLモデム)、3…DSLAM、4…ATMスイッチ (交換機)、5-1, 5-2, 5-3…NSP、6…VSG、7…BAS、81, 82…VPN選択接続ゲートウェイ (VSG)、9…アクセス網、10…コア網、6-1…DHCPサーバ機能、6-2…HTTPサーバ機能、6-3…Radius Client機能、6-4…DNSサーバ機能、6-5…SA-VR対応テーブル、6-6…VR、6-7…アドレス変換テーブル (プライベート側)、6-8…アドレス変換テーブル (グローバル側)、6-9…ARPテーブル、5-1-2…NSP側のDNSサーバ。

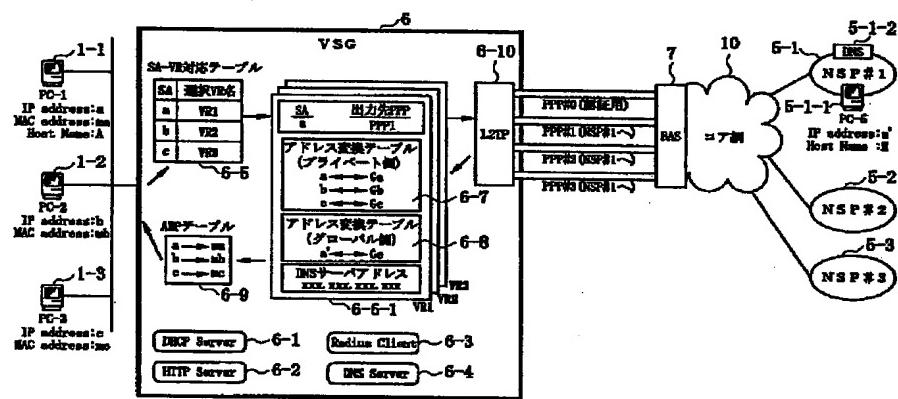
【図1】



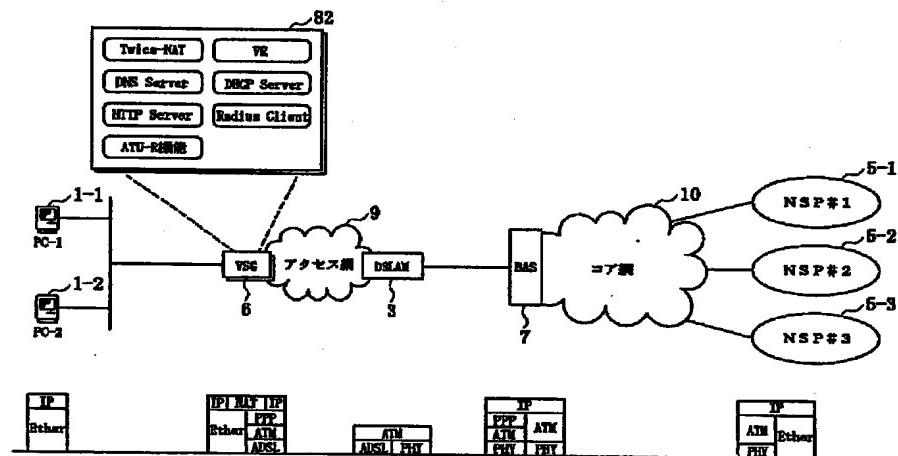
【図 2】



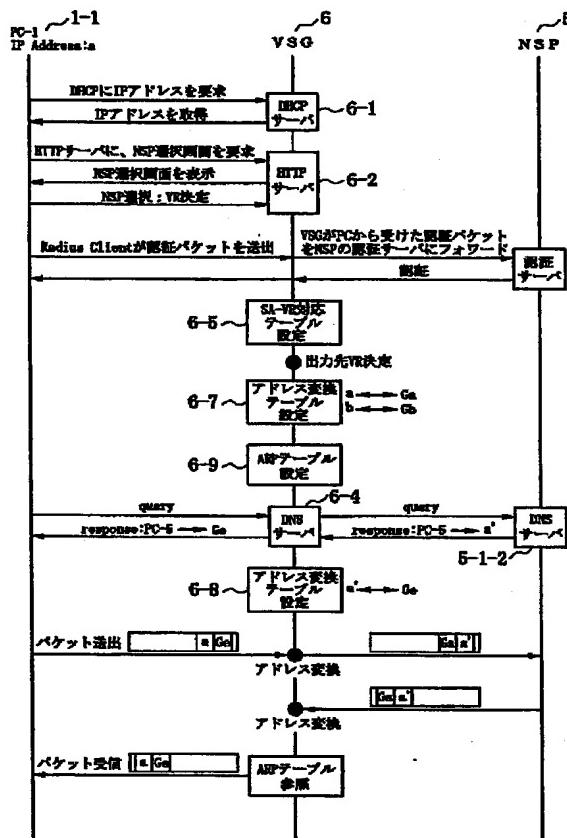
【図 3】



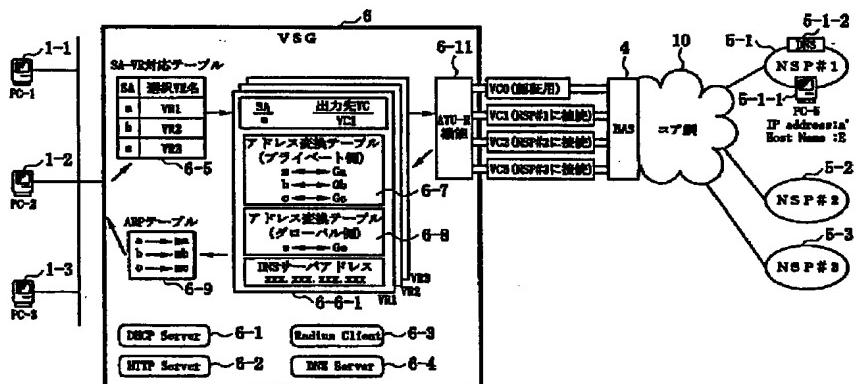
【図 5】



【図 4】



【図 6】



フロントページの続き

(72)発明者 早瀬 千善
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

Fターム(参考) 5J104 AA07 KA02 MA01 NA05 PA07
5K030 GA11 HA08 HA10 HC01 HC14
HD03 HD06 HD09 JT06 LB06
5K033 AA09 BA15 CB09 CC01 DA06
DB18 EC03
9A001 CC03 CC06 CC08 DD10 DD13
EE03 JJ25 JJ27 KK56